



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/896,197	06/29/2001	Petrus Lambertus Adriaanus Roelse	NL000365	7563

24737 7590 04/05/2005

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER

SHIFERAW, ELENI A

ART UNIT PAPER NUMBER

2136

DATE MAILED: 04/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary**Application No.**

09/896,197

Applicant(s)ROELSE, PETRUS LAMBERTUS
ADRIAANUS**Examiner**

Eleni A Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 June 2001.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Final rejection

1. Applicant's arguments/amendments with respect to the amended claims 1, 3, 5-8, 10-11, and 13, original claims 2, 4, 9, and 12, and added claims 14-20 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Heys, et al. "The Design of secure Block Ciphers", May 1994.

As per claim 1, Heys teaches a method for cryptographically converting an input data block into an output data block; the method including performing:

selecting a select permutation from a predetermined set of at least two permutations (page 1 par. 1 & 5 and page 3 last paragraph); and

performing a non-linear substitution operation on the input data block based on the select permutation (page 1 par. 1 & 5 and page 3 last paragraph).

As per claim 13, Hays teaches a system for cryptographically converting an input data block into an output data block; the system including:

- an input for receiving the input data block (page 3 last paragraph, page 5 first paragraph);
- a storage for storing a predetermined set of at least two permutations associated with an S-box (page 4 paragraph 8);
- a cryptographic processor for performing a non-linear operation on the input data block using an S-box based on a permutation (page 1 par. 1 & 5 and page 3 last paragraph);
- the processor being operative to, each time before using the S-box, (pseudo-)randomly selecting the permutation from the stored set of permutations associated with the S-box (page 1 par. 1 & 5, page 2 par. 3, page 3 last paragraph, and page 6 par. 5-6); and
- an output for outputting the processed input data block (page 3 last paragraph).

As per claim 14, Hays teaches a cryptographic encoder comprising:

- one or more encryption stages (page 4 par. 8-9),
- each stage of the one or more encryption stages including
 - a non-linear substitution module that is configured to receive a control signal and a set of data bits (page 1 last paragraph),
 - wherein the non-linear substitution module includes a plurality of substitution boxes (page 1 last paragraph); and
 - each of the substitution boxes is configured to receive at least a subset of the control signal and a subset of the set of data bits (page 1 last paragraph), and:

substitutes a first output value for the subset of the set or data bits if the subset of the control signal is a first value (page 1 abstract & last paragraph, page 2 par. 3, and page 3-4 No. IV), and

substitutes a second output value for the subset of the set of data bits if the subset of the control signal is a second value (page 1 abstract & last paragraph, page 2 par. 3, and page 4-5 No. V).

As per claim 2, Hays teaches a method, wherein the set of permutations is formed such that a cryptographic weakness in one of the permutations of the set is at least partially compensated by a corresponding cryptographic strength in at least one of the other permutations of the set (page 1 abstract and page 3-4 No. IV).

As per claim 3, Hays teaches a method, wherein

the data block consists of n data bits (page 2 par. 3), and
each permutation of the set of permutations is a set of $2^{\sup n}$ elements, represented by,
where each non-trivial differential characteristic of each permutation in this set has a probability that is less than or equal to a maximum probability (page 3 last paragraph),

the set of permutations being formed by permutations which have been selected such that for each non-trivial differential characteristic having the maximum probability in any of the permutations, this differential characteristic has a lower probability in at least one of the other permutations of the set (page 3 last paragraph and page 2-3 No. III).

Art Unit: 2136

As per claim 4, Hays teaches a method, wherein the differential characteristic has a probability equal to zero in at least one of the permutations (page 2-3 No. III and page 3 No. IV).

As per claim 5, Hays teaches a method, wherein $n=4$, and the maximum probability equals $\frac{1}{4}$ (page 3 No. IV).

As per claim 6, Hays teaches a method, wherein

the data block consists of n data bits (page 2 par. 3), and

each permutation of the set of permutations is a set of $2^{\sup n}$ elements, where each non-trivial linear characteristic of each permutation in this set has a probability of at least minimum probability and at most maximum probability (page 3 last paragraph),

the set of permutations being formed by permutations which have been selected such that for each non-trivial linear characteristic with probability that equals the minimum or maximum probability in any of the permutations, this linear characteristic has a probability closer to $\frac{1}{2}$ in at least one of the other permutations of the set (page 4 par. 15).

As per claim 7, Hays teaches a method, wherein the linear characteristic has a probability equal to $\frac{1}{2}$ in at least one of the permutations (page 4 par. 15).

As per claim 8, Hays teaches a method, wherein $n=4$, the minimum probability is $\frac{1}{4}$ and the maximum probability is $\frac{3}{4}$ (page 3-4 No. IV).

As per claim 9, Hays teaches a method, wherein the set of permutations consists of two permutations (page 3-4 No. IV).

As per claim 10, Hays teaches a method, wherein
selecting the select permutation is based on an encryption key (page 1 abstract and last paragraph).

As per claim 11, Hays teaches a method, wherein
selecting the permutation is performed under control of a bit of an encryption key (page 2 No. II).

As per claim 15, Hays teaches the cryptographic encoder, wherein
each stage of the one or more encryption stages further includes
an addition module that is configured to combine at least a subset of a key
with a data input to provide the set of data bits to the non-linear substitution module (page 1 abstract and page II No. II).

As per claim 16, Hays teaches the cryptographic encoder, wherein
the control signal includes another subset of the key (page 2 par. 3).

As per claim 17, Hays teaches the cryptographic encoder, wherein
each stage of the one or more encryption stages further includes
a transformation module that is configured to transform the output values from

the substitution boxes to provide therefrom an encrypted data output (page 3-4 No. IV).

As per claim 18, Hays teaches the cryptographic encoder, wherein

the second output value is formed such that a cryptographic weakness in the first value is at least partially compensated by a corresponding cryptographic strength in the second output value (page 1 abstract).

As per claim 19, Hays teaches the cryptographic encoder, wherein

the subset of the set of data bits consists of n data bits (page 2 par. 3), and each of the first and second data output values is a mapping of the subset of the set of data bits to an element of a set of 2^n elements, where each non-trivial differential characteristic of each of the set of 2^n elements of the first and second output values has a probability that is less than or equal to a maximum probability (page 3 last paragraph);

the set of 2^n elements that provide second data output value being selected such that for each non-trivial differential characteristic having the maximum probability in the set of 2^n elements that provide the first output value, this differential characteristic has a lower probability in the set of 2^n elements that provide second data output value (page 3 last paragraph and page 2-3 No. III).

As per claim 20, Hays teaches the cryptographic encoder, wherein

the subset of the set of data bits consists of n data bits (page 2 par. 3), and each of the first and second data output values is a mapping of the subset of the set of data bits to an element of a set of 2^n elements, where each non-trivial differential characteristic

of each of the set of 2^n elements of the first and second output values has a probability that is at least a minimum probability and at most a maximum probability (page 3 last paragraph);

the set of 2^n elements that provide second data output value being selected such that for each non-trivial linear characteristic that equals the minimum or maximum probability in the set of 2^n elements that provide the first output value, this linear characteristic has a probability closer to $1/2$ in the set of 2^n elements that provide second data output value (page 4 par. 15).

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

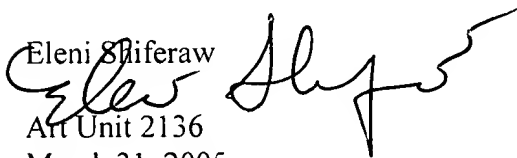
Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw

Art Unit 2136
March 31, 2005


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100